مقالات من مشروع كلاين

مفتاح الشـفرة العمومي

بقلم : **أنتوان نكتو** Antoine Nectoux

ترجمة : أسماء تراوش

المؤلفون الأصليون : **غريم. ل. كوهن** Graeme L. Cohen (جامعة التكنولوجيا، سيدني Sydney)، **ستيفن غالبريث** Steven Galbraith (جامعة أوكلاندا Auckland)، **إدواردو برسيشتي** Edoardo Persichetti (جامعة أوكلاندا).

كيف نستطيع إرسال تفاصيل بطاقتنا الائتمانية عبر الانترنت، أو باستعمال الهاتف النقال، في الوقت الذي يستطيع فيه آخرون اعتراض رسائلنا؟ كيف نستطيع أن نثق في برامجيات التحديث، ونحن على علم بانتشار الفيروسات الحاسوبية؟ التشفير، أو التعمية Cryptography (دراسة تقنيات التواصل الآمن في حال وجود خصوم وأعداء) يزودنا بأجوبة عن هذه الأسئلة، والرياضيات تمدّنا بأساسياته.

لمحة تاريخية

منذ آلاف السنين كان التواصل بطريقة آمنة وسرية محل اهتمام : هناك ما يدل على أن يوليوس قيصر Julius Caesar استعمل طريقة تشفير بسيطة للتواصل مع قادة جيوشه. وتُعرف هذه الخطة باسم "شفرة قيصر" التي تقوم على إجراء نفس الإزاحة لكل حرف بعدد معين من المرات ليشغل موضعا جديدا في الرسالة. وبذلك نحصل على وثيقة تدعى بـ"النص المشفر" ciphertext. يمكن للطرف الثاني (مستقبل البرقية) استعادة النص الأصلي للرسالة عند إجراء العملية العكسية، أي بجعل الحروف في النص تنزاح في الاتجاه الآخر بنفس عدد المرات التي تبناها المشفّر.

جوهر الفكرة يتمثّل في كون كلّ من المرسل والمستقبل ينبغي أن يكونا على علم بقيمة سرية (في هذه الحالة، القيمة السرية هي عدد الوضعيات) التي من المفترض أن تكون غير معروفة لدى الأطراف الأخرى الساعية إلى الاطلاع على فحوى البرقية. تدعى القيمة السرية بالمفتاح (key). في حالة شفرة قيصر فإن المفتاح K هو عدد محصور بين 0 و 26. تأخذ خوارزمية التشفير Enc كمدخل رسالة M (Message) ومفتاح K. مثال ذلك : $\mathrm{Enc}_3(\mathrm{HELLO}) = \mathrm{KHOOR}$. أما عملية فك الشفرة Dec فتتخذ كمدخل لها النص المشفرة C ونفس المفتاح K. مثال ذلك : $\mathrm{Dec}_3(\mathrm{KHOOR}) = \mathrm{HELLO}$.

تدعى أنظمة التشفير التي تستعمل فيها نفس المفتاح لوضع شفرة وفكها أنظمة المفتاح التناظري.

تعتبر شفرة قيصر بسيطة جدا ولذا لا يمكنها أن تكون آمنة في عصرنا الحالي. غير أنه توجد شفرات بمفاتيح تناظرية ذات استعمال واسع في كثير من الوضعيات؛ كمثال على ذلك هناك الشفرة الشهيرة AES، وهي أحد معايير نقل المعلومات لدى الحكومة الأمريكية. ورغم فعالية وأمان هذه الأنظمة فإنها تطرح مشكلا : على كل من المرسل والمستقبل أن يتقاسما مسبقا سرّا معينًا. فكيف لنا إذن أن نتواصل عبر الإنترنت بطريقة آمنة مع أناس لم نلتق بهم أبدا؟

فكان الحل لهذا المشكل في ظهور مفهوم مذهل عرف باسم "مفتاح الشفرة العمومي" الذي صدر لأول مرة سنة 1976 ضمن بحث بعنوان "اتجاهات جديدة في الشفرة" (New directions in cryptography) بقلم وايتفيلد ديفي Whitefield Diffie ومارتن هلمن Martin Hellman.

في هذه الحالة، عوضًا عن استعمال مفتاح واحد لوضع شفرة وفكها، نستعمل مفتاحا عموميا متاحا لجميع المستعملين، ومفتاحا خاصا يظل سريًا لمستعمل معيّن. بعبارة أخرى فالكل يستطيع أن يبعث برسالة، لكن هناك شخصا واحدا فقط يمكن تلقيها : كلٌّ منا يستطيع وضع رسالة عبر شق صندوق بريد، غير أنه لا يوجد سوى شخص واحد يمكنه الحصول عليها، وهو الشخص الذي يمتلك مفتاح صندوق البريد. للتواصل بأمان مع أليس Alice يقوم أحدهم بالبحث عن مفتاحها السري ويستعمله لإنشاء نص مشفر لا يستطيع فكه إلا أليس لأنها الوحيدة التي تعرف المفتاح الخاص السري.

ينبغي على أنظمة التشفير أن تقوم على المسائل الحسابية المتميزة بصعوبة الحل. تزودنا الرياضيات بمثل تلك المسائل. نشير كمثال على ذلك إلى نظام RSA القائم على صعوبة التوصل إلى العوامل الأولية لعدد صحيح كبير جدا.

نبذة عن نظرية الأعداد

قبل وصف مفتاح الشفرة العمومي RSA الذائعة الصيت نحتاج إلى بعض نتائج نظرية الأعداد. وهذا ما يتطلب الإلمام بمبرهنة ثنائي الحد وبالحساب الترديدي (أو المقاسي) modular arithmetics إلماما متواضعا.

في الحساب الترديدي نجمّع الأعداد الصحيحة في صفوف حسب باقي قسمتها على عدد معين p، يدعى ترديد modulus. فعلى سبيل المثال، إذا كان $p=7$ فإن لدينا 9 في صف 2. كما أن 5، 12، 19 أعداد تنتمي إلى نفس الصف. ونكتب $9\equiv 2 \pmod 7$ و $12\equiv 19\equiv 5 \pmod 7$. من السهل ملاحظة أنه توجد فقط سبعة صفوف ممكنة، ممثلة بالمجموعة $\{0,1,2,3,4,5,6\}$ عندما نعمل بترديد 7. إنه بالإمكان إجراء عمليتي الجمع والضرب بترديد 7 وهذا يتم ببساطة عند القيام بطرح مضاعف الترديد إثر القيام بالعملية وفق القواعد المعتادة. وهكذا : $3+8=11\equiv 4 \pmod 7$ و $3\times 5=15\equiv 1 \pmod 7$. لاحظ أنه إذا كان $a\equiv b \pmod p$ فإن $(a-b)$ سيكون مضاعفا لـ p.

ليكن p و q أوليين حيث $p\neq q$، وليكن $t>0$ عددا صحيحا ليس مضاعفا لـ p أو q. سنبين الآن أن العلاقة $t^{(p-1)(q-1)}\equiv 1 \pmod{p.q}$ قائمة. تمثل هذه العلاقة حالة خاصة من مبرهنة فيرما–أولر Fermat-Euler.

البرهان يبدأ بصيغة ثنائي الحد:

$$\binom{p}{i}=\frac{p!}{i!(p-i)!}$$

حيث i عدد طبيعي $0<i<p$. ينتج من

$$i!\binom{p}{i}=p(p-1)(p-2)...(p-i+1)$$

أنه على p أن يكون قاسما لـ $\binom{p}{i}$، ذلك لأن p يقسم الطرف الأيسر ولا يقسم $i!$.

ومن ثمّ، فمن أجل كل عددين صحيحين A و B، وبمراعاة مبرهنة ثنائي الحد، نحصل على :

$$(A+B)^p=A^p+\binom{p}{1}A^{p-1}B+\binom{p}{2}A^{p-2}B^2+...+B^p\equiv A^p+B^p \pmod p.$$

وباعتبار عدد طبيعي آخر C يأتي :

$$(A+B+C)^p=((A+B)+C)^p\equiv (A+B)^p+C^p\equiv A^p+B^p+C^p \pmod p.$$

بهذه الكيفية نحصل من أجل كل أعداد صحيحة A_1 ، A_2 ، ...، A_t على :

$$(A_1+A_2+...+A_t)^p\equiv A_1^p+A_2^p+...+A_t^p \pmod p.$$

والآن بوضع $A_1=A_2=...=A_t=1$ يتضح أن

$$t^p\equiv t \pmod p.$$

بما أن $(t^p-t)=t(t^{p-1}-1)$ فالمعادلة السابقة تعني أن العدد $t(t^{p-1}-1)$ مضاعف لـ p.

نعلم (فرضا) أن t ليس مضاعفا لـ p. في هذه الحالة لما كان p أوليا فإن :

$$t^{p-1}\equiv 1 \pmod p$$

والآن، برفع كلٍ من طرفي الموافقة إلى القوة $q-1$ يتضح أن :

$$t^{(p-1)(q-1)} \equiv 1 \pmod{p}.$$

وبتكرار نفس العملية بعد استبدال p بـ q نحصل على :

$$t^{(p-1)(q-1)} \equiv 1 \pmod{q}.$$

هذا معناه أنه يوجد عددان طبيعيان h و k يحققان على الترتيب : $t^{(p-1)(q-1)} = 1 + ph$ و $t^{(p-1)(q-1)} = 1 + qk$. ولذلك فإن : $ph = qk$.

ومنه p يقسم k (لأن p و q عددان أوليان مختلفان). وبالتالي $k = pl$ حيث l عدد طبيعي. وهكذا نصل إلى العلاقة $t^{(p-1)(q-1)} \equiv 1 + pql$، أي $t^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. وهذا ما ينهي البرهان □

نظام التشفير RSA

RSA هو الحروف الأولى لأسماء الأعلام الثلاثة : ريفست Rivest، شمير Shamir، أدلمان Adleman الذين كانوا أول من اقترحوا هذا النظام عام 1977. يعمل هذا النظام كالتالي.

أولا، اختر عددين أوليين مختلفين p و q، ثم احسب $N = pq$ و $\phi = (p-1)(q-1)$. ثم اختر عددا طبيعيا كيفيا e محصورا بين 3 و $N-2$ بحيث لا يكون لـ e و ϕ عوامل أولية مشتركة بينهما. المفتاح العمومي عندئذ هو الثنائية (N,e). أما المفتاح الخاص d الذي سيبقيه المرسل سرًا، فينبغي أن يحقق العلاقة $d \equiv e^{-1} \pmod{\phi}$. ومن ثم $de \equiv 1 \pmod{\phi}$ (نحصل على هذه نتيجة بسهولة باستعمال خوارزمية إقليدس). فعلى سبيل المثال، بأخذ $N = 437 = 19.23$ يكون $\phi = 369$، وباختيار $e = 5$ يكون $d = 317$ (تلك هي أصغر قيمة يأخذها d).

إن الرسائل في نظام RSA أعداد طبيعية x بحيث $0 < x < N$. في البداية قد لا تكون عملية تشفير نصوص الرسائل بواسطة مخطط يستعمل الأعداد الطبيعية عملية واضحة. ومع ذلك فإن أنظمة التشفير المطبقة في أجهزة الحاسوب وفي جميع الملفات ممثلة كلها في معطيات كتبت بنظام ثنائي، يمكن تشفيرها بواسطة الأعداد الطبيعية.

عملية التشفير هي الآتية. نفرض أن بوب يريد أن يبعث برسالة x إلى أليس. من أجل ذلك يبحث عن مفتاحها العمومي (N,e). ثم يحسب $y \equiv x^e \pmod{N}$، ويرسل بعد ذلك y إلى أليس. لفك رموز النص المشفر y، تستعمل أليس المفتاح الخاص d، عن طريق حساب $x \equiv y^d \pmod{N}$. من المهم الإشارة إلى أنه رغم كبر الأعداد e، d، N فإننا نستطيع أن نقوم بالحسابات بسلاسة، فمثلا لحساب $y^d \pmod{N}$ نستعمل تقنية تسمى الأسّية الترديدية Modular exponentiation .

نستطيع القيام بعملية فك الشفرة مادام $de = 1 + k\phi$، من أجل عدد صحيح k، علما أن (كما بينا أعلاه):

$$x^{\phi} = x^{(p-1)(q-1)} \equiv 1 \pmod{N}$$

(في الواقع يمكننا تجاهل الحالة التي يكون فيها x مضاعفا لـ p أو q)، ولذا فإن :

$$y^d \equiv (x^e)^d = x^{1+\phi k} = x(x^\phi)^k \equiv x.1^k = x \pmod N .$$

الملاحظ أن المستعمل الدخيل الذي لا يعرف المفتاح الخاص d، ينبغي عليه تفكيك N إلى جداء عوامل أولية لاكتشاف العددين P و q. وهذه العملية تتجاوز طاقة الحواسيب المتداولة إذا ما كانت الأعداد الأولية المطلوبة كبيرة بكفاية، يفوق عدد أرقام كل منهما 200 رقم مثلا (الأرقام القياسية العالمية في موضوع التفكيك إلى عوامل أولية تشير إلى أنه يمكن تحليل $N = p.q$ عندما يتكون كل من العاملين من نحو 100 رقم لا أكثر).

وهذا في الحقيقة ما يحدد مستوى الحماية للنظام. فالفكرة المحورية لمفتاح الشفرة العمومي هي أنه، طالما تبوء محاولات المصادر الهجومية لاختراق الحواسيب بالفشل فهذا يدل على أن نظام التشفير في أمان. هذا الأمر يحدد مسبقا (عادة ما يكون 2^{128} أو 2^{256} عملية أنمولية)، كما أن هذا الموضوع مرتبط بسياق وهدف الاتصال. فمن الواضح أن رسالة سرية لوكالة الاستخبارات المركزية الأمريكية وبريد إلكتروني بين مستخدميْن لشبكة الانترنت لا نتوقع أنهما يتمتعان بنفس معايير للحماية !!!

التوقيعات

يمكننا الآن الرجوع إلى مشكل تحديث البرامج، أي مشكل التوثيق. فكما أسلفنا، لدينا مفتاح عمومي ومفتاح خاص. تستعمل أليس مفتاحها الخاص لإنشاء توقيع رقمي ليرسل مع وثيقة حتى يثبت موثوقيتها (التوقيع مرتبط بالوثيقة ولا يمكن قصه وإلصاقه في وثيقة أخرى). عندئذ يقوم المستقبِل بالتحقق من هذا التوقيع مستعملا المفتاح العمومي .

لنفرض مثلا، أن حاسوبك أظهر لك أنه وجد برنامج تحديث لـ"أدوب" Adobe. فكيف له أن يعرف أن هذا برنامج تحديث وليس فيروسا في هيئة برنامج؟ الحل يكمن في أن يمتلك برنامج التحديث توقيعا رقميا بالنسبة للمفتاح العمومي لـ"أدوب". فذلك المفتاح مثبت قبل اليوم على حاسوبك في برنامج "أدوب". ومن ثمّ يمكن للحاسوب أن يتحقق من التوقيع قبل القيام بتثبيت المستجدات. وهكذا فنجاح عملية التحقق يؤكد لنا أن مصدر البرنامج هو "أدوب" وليس مصدرا آخر.

دعنا نوضح الآن كيف ننشئ توقيعا رقميا باستعمال RSA.

الملاحظ أن كلاً من المفتاحين العمومي والخاص يتعلق بعملية التشفير. عندما تريد أليس التحقق من وثيقة (مثال: برنامج تحديث) فما عليها سوى تحويلها إلى عدد طبيعي x حيث $0 < x < N$، ثم حساب $\sigma \equiv x^d \pmod N$، وبعدها ترفق التوقيع σ بالملف. أما بوب فيقوم بالتحقق من التوقيع بحساب $x' \equiv \sigma^e \pmod N$، ثم التأكد من المساواة $x = x'$. من الجلي، كما هو الحال في نظام التشفير *RSA*، أنه إذا حاول دخيل إنشاء توقيع مُجْدٍ (مثلا: قرصان يريد تصميم فيروس) فسيحتاج إلى معرفة الأس d، الأمر الذي يتطلب البحث عن تفكيك N إلى عوامل أولية.

البحوث الحالية

لقد عرّفنا بنظام تشفير RSA وأنظمة التوقيع الرقمي للبرامج، غير أن هناك عدة أنظمة أخرى قائمة على مواضيع مختلفة في الرياضيات، مثل: الحقول المنتهية، والمنحنيات الناقصية، وجملة المعادلات غير الخطية المتعددة المتغيرات، رموز تصحيح الخطأ وغيرها.

إن مفتاح الشفرة العمومي مجال بحث جد نشط، ولا زالت هناك أسئلة مفتوحة قيد الدراسة.

سيناريو ما بعد الكمي

هل كل مشاكلنا تحل بـ RSA؟ لسوء الحظ فالإجابة هي بالنفي. ذلك أن أمان هذا النظام كغيره من المخططات القائمة على نظرية الأعداد مهدد بصفة جدية من جراء التطور الهائل الذي تسجله الحواسيب الكمومية. فخوارزمية شور Shor –التي ظهرت سنة 1994 تحت العنوان الواعد "*Polynomial time algorithms for discrete logarithms and factoring on a quantum computer*" قادرة على التفوق على نظام تشفير RSA إذا ما تواصلت صناعة الحواسيب الكمومية على نطاق واسع. هناك حواسيب كمومية صغيرة الحجم أصبحت متوفرة الآن ومن المنتظر أن تعرف تحسينات في المستقبل القريب.

لذلك فمن المهم دعم الأنظمة البديلة القادرة على مقاومة آثار هذا السيناريو إذا ما أصبح حقيقة. والملاحظ أن المعنيين بالتشفير نشطون جدا في هذا الاتجاه، وهناك بحوث جارية تركز على تطوير أنظمة تشفير جديدة مبنية على فروع مختلفة من الرياضيات. وهذه الأنظمة قائمة على مسائل حسابية نأمل أنها لن تعاني من نفس نقاط الضعف أمام الخوارزميات الكمومية.

المراجع

[1] Simon Singh, The Code Book : *The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (2000), Anchor.

هذا المقال متوفر أيضا بـ: الانجليزية، الفرنسية، الألمانية، الاسبانية.